(U) Giving Answers, Keeping Secrets

FROM: [redacted]
Acting Chief of Operations, Yakima Research Station (YRS)
Run Date: 12/05/2006

(S//SI//REL) New query tool, VIVIDDREAM, tells whether a VPN session is likely exploitable -- without revealing any close-hold information.

SERIES:
(U) SIGDEV Collaboration

1. [redacted]

(S//SI//REL) Ever hear the phrase, "It's so secret that if I told you, I'd have to kill you"? This may be rather extreme, but when dealing with Virtual Private Networks* (VPNs) in the field, it captures some of the challenges of being away from NSA-W. Exploiting VPNs makes use of some of the newest state-of-the-art techniques and because of this, the exploitation details are held closely and generally not available to field sites. When VPNs were discovered at Yakima Research Station (YRS), a time-consuming manual process was required that involved analysts from both YRS and NSA-W's Cryptanalysis and Exploitation Services (CES) to determine the likely exploitability of a given network. This process generally involved forwarding data from field survey traffic and an analyst-to-analyst exchange of information. Frustration was often the result when it was found that the time and effort spent had been for a network that was not, in fact, likely exploitable.

(S//SI//REL) Analysts at Yakima Research Station dreamed of a magic box that could accept information about a network and give a simple yes or no answer as to whether a VPN session might be exploited and to obtain that answer without revealing any sensitive information. Such a shortcut would assist with the network "triage" that frequently must take place in the field: A yes could tag a network for possible exploitation and a no could mark a network for further study. This magic box is precisely what YRS created in the form of the VIVIDDREAM query tool.

(S//SI//REL) The VIVIDDREAM query tool automatically sends metadata about a collected VPN to VIVIDDREAM, a Cryptographic Exploitation Services database, and returns only a positive or negative response. Since a definitive answer based on the limited metadata is impossible, CES analysts have been striving to educate query tool users on the interpretation of often ambiguous responses. While the query tool offers an analyst performing VPN SIGDEV a glimpse into the possibilities of VPN exploitation, direct interaction with CES is still necessary to proceed with exploitation of a target's VPN communications.

(S//SI//REL) The VIVIDDREAM query tool treads the delicate line between protecting VPN exploitation capabilities and enabling VPN SIGDEV to proceed. The developers took care to make the tool shareable across the SIGINT enterprise and to promote its use. It was featured at the VPN boot camp at NSA-Hawaii and briefed at the annual SIGDEV conference in June 2006. This marketing push has been effective and has resulted in over seventy downloads from the YRS software sharing site. With the use of the VIVIDDREAM query tool from both the field and NSA-W elements,

significant time is saved and sensitive information is given the protection it requires.

(U//FOUO) For more information about VIVIDDREAM and the YRS-developed query tool, type " go vividdream " in your intranet browser or contact [redacted], F921C [redacted] or [redacted] S31213 [redacted].

---

*(U) Note: For some background info on VPNs, see an earlier SIDtoday article, " Efforts Against Virtual Private Networks Bear Fruit. "
